

IPsec Panel:

Issues and Challenges in Implementing IPsec

IPsec is a suite of protocols and algorithm standards developed in the IETF and adopted as Internet standards to provide authentication, integrity, and privacy for information sent across IP networks. By operating at the IP layer, it can afford protection for any type of traffic carried over IP. Moreover, this layering allows IPsec security associations to operate on a true end-to-end basis, or to be terminated at security gateways (e.g., firewalls), allowing flexible deployment for the technology. IPsec can be employed in both intranet and extranet contexts. This panel will discuss the issues and challenges involved in implementing the IPsec protocol suite and the lessons learned.

Chair:

Steve Kent
BBN Technologies
Chief Scientist- Information Security, BBN Technologies;
Director, Security Practice Center, GTE Internetworking;
Chief Technical Officer, CyberTrust Solutions
MS 13/2A
70 Fawcett Street
Cambridge, MA 02138
kent@bbn.com

Dr. Stephen T. Kent
Chief Scientist- Information Security, BBN Technologies
Director, Security Practice Center, GTE Internetworking
Chief Technical Officer, CyberTrust Solutions

In his role as Chief Scientist, Dr. Kent provides oversees information security activities within BBN Technology, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of several network security systems for the Department of Defense and served as principal investigator on a number of network security R&D projects for almost 20 years. As Director of the SPC, Dr. Kent monitors all security-related aspects of the service offerings of GTE Internetworking Services. He reports to the President of GTE Internetworking and coordinates with engineering, operations, and marketing to ensure the security quality of offerings. As CTO for CyberTrust Solutions, Dr. Kent provides strategic direction for this certification authority business, reporting to the General Manager of CyberTrust.

Over the last 20 years, Dr. Kent's research and development activities have included the design and development of user authentication and access control systems, network-layer encryption and access control systems, secure transport-layer protocols, secure e-mail

technology, multilevel secure (X.500) directory systems, public-key certification authority systems, and key recovery (key escrow) systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications, security for Internet routing, and security for mobile computing.

The author of two book chapters and numerous technical papers on network security, Dr. Kent has served as a referee, panelist and session chair for a number of conferences. Since 1977 he has lectured on the topic of network security on behalf of government agencies, universities, and private companies throughout the United States, Europe, Australia, and the Far East. Dr. Kent received the BS degree in mathematics from Loyola University of New Orleans, and the S.M., EE, and Ph.D. degrees in computer science from the Massachusetts Institute of Technology. He is a Fellow of the ACM, a member of the Internet Society and Sigma Xi, and appears in *Who's Who in the Northeast* and *Who's Who of Emerging Leaders*.

Panel Members:

Cheryl Madson
Cisco Systems, Inc.
170 W. Tasman Dr.
San Jose, CA 95134
408/527-2817
cmadson@cisco.com

Cheryl Madson is a Senior Software Engineer in the IOS Network Protocols/Security group at Cisco Systems, Inc. She has been an active member of the IETF's IPsec Working Group for several years, and has helped to implement IPsec for Cisco's router platform.

She has worked in the areas of IP-based networking and/or communications security since 1983. Previous development projects have included the (Wang Labs) Trusted Interface Unit (a standalone high-grade IP-layer encryption unit), a proprietary protocol-to-MILNET protocol gateway, and IP multicast routing.

She received her BS in Quantitative Methods and Information Systems from St. Cloud State University (MN) in 1981, and an MS in Software Design and Development from the University of St. Thomas (St. Paul, MN) in 1987.

Naganand Dormaswamthy
Bay Networks
(978)916-1323 (O)
Bay Architecture Lab
(978)916-0620 (Fax)
3 Federal St, Mail Stop BL3-03
Billerica, MA 01821

naganand@BayNetworks.COM

Naganand Doraswamy works for Bay Networks in the architecture lab. He is currently working on architecture and design of high speed routers and security architectures. He chaired the VPN BOF at the IETF and is the working group chair for IP Payload Compression. His interests include Internetworking Architectures and Security. He architected and implemented IPsec while at FTP Software.

Roy Periera
TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario
K2K 2P5 Canada
1-(613)-599-3610 x4808
rpereira@timestep.com

Roy Pereira is the Security Architect with TimeStep Corporation, an affiliate company of Newbridge Networks. At TimeStep, he is heavily involved with security and Internet standards as well as product direction, new technology, product integration and product management. He has been an active member and an author in IETF's IPsec Working Group. Mr. Pereira has 11 years experience in the software development industry and has been involved with Internet protocols for 9 years.